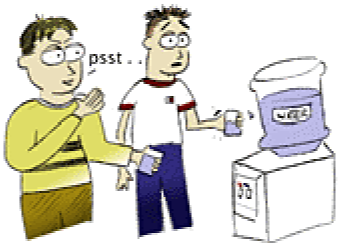
Security Quickie 6

This week's Security Quickie: Trusted Sources of Information



With today's technology, we can communicate ideas and information with astounding speed. We can check our e-mail, chat with friends, or browse the news with just a few clicks of our mouse. When the information we receive isn't entirely accurate, however, we can receive or propagate that bad information just as quickly.

The spread of rumors, panic, and misinformation can easily become a drain on state resources and employee time and morale. Trust those sources of information that are authorities in their field, and be cautious in trusting those that aren't. For information security issues use resources such as SANS, Security Focus, product vendors, and ITD's Information Security Office. (Some of these resources are linked via the ISO website http://www.itd.state.ia.us/security/ in the Education - Links section) News services are **not** the best source of security information because they are mainly interested in being the first to get a story out, not in the story's accuracy. Internet friends who are "in the know" may not have received their facts from trusted sources or may only understand part of a given issue.

When receiving or reading security news and information use common sense and verify the information with a trusted source. While your friends may be a trusted source of information on many topics, ask yourself what their training is and whether they really are an expert or just passing an opinion. Just because someone appears to have knowledge about a subject doesn't mean they *are* knowledgeable (this is known as false autority syndrome). While many people may have a great deal of experience with PC issues, few of them are really qualified to alert you about virus dangers or are a definitive authority on the dangers of computer crime. By acting on or passing along misinformation and inaccurate information we can easily become part of the problem instead of part of the solution.

A couple tips to avoid current hoaxes:

Virus hoaxes are not always easily discernable. Check with your appropriate departmental personnel (your security specialist or ITD's Information Security Office) before disseminating information about viruses and other malicious code. You can also check at sites such as Virus Myths homepage (www.vmyths.com) or McAfee's hoax website (<http://vil.mcafee.com/hoax.asp>) to research documented hoaxes.
Also, most hoaxes have the following characteristics:

- They tell of catastrophic damage ("This will eat your hard drive!")
- Lots of ALL CAPS and explanation points!!!!!
- They ask you to send it everybody you know.
- They site sources such as AOL and IBM. These are not normal sources for virus alerts.

Regarding patches, Microsoft (and other vendors) **never** e-mail patches, only announcements of updates and patches. Administrators and users must currently visit Microsoft's security update site (windowsupdate.microsoft.com) to obtain system updates. Microsoft also has their TechNet site (http://www.microsoft.com/technet/security/), which has the latest patches, news, and informative articles regarding their products. The main point is that vendors do not mass-mail patches; you need to visit trusted vendor sites to get viable patches and updates